



Centrálny depozitár cenných papierov SR, a. s.

**Executory Decree No. 1
to the Rules of Operation of Centrálny depozitár
cenných papierov SR, a.s.**

**COMMUNICATION OF THE PARTICIPANT
WITH IS CDCP**

Centrálny depozitár cenných papierov SR, a.s.
ul. 29. Augusta 1/A, 814 80 Bratislava I
registered in the Commercial Register of the District Court Bratislava I VAT ID: SK2020312833
section: Sa, insert No. 493/B
Phone: 00421/2/59395110

Business ID: 31 338 976
Tax ID: 2020312833
www.cdcp.sk
Fax: 00421/2/ 5296 8755

Bank details
TATRA BANKA, a.s.
IBAN: SK87 1100 0000 002622003416
BIC: TATRSKBX

Table of content

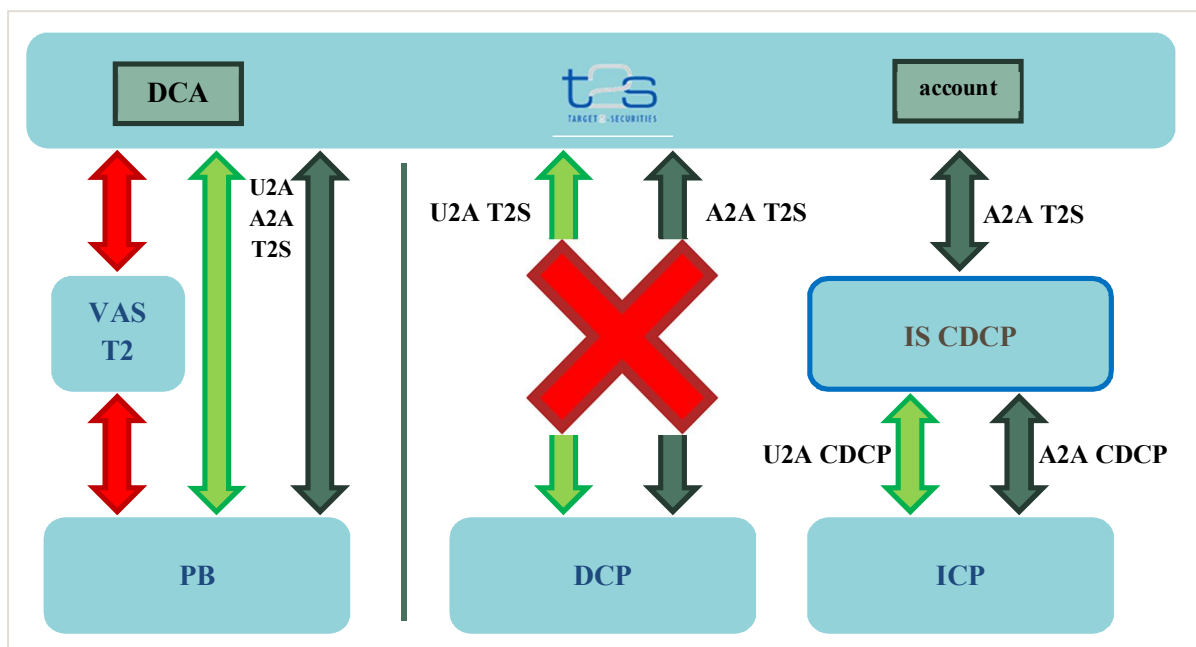
1	INTRODUCTION	3
2	GENERAL VIEW	3
3	OPTIONS OF CONNECTION TO THE IS CDCP	4
3.1	U2A MODE.....	4
3.2	A2A MODE.....	5
4	TECHNICAL REQUIREMENTS FOR THE PARTICIPANT	5
4.1	U2A MODE.....	5
4.2	THE A2A MODE – WEB SERVICES	6
4.3	A2A – SWIFT MODE	7
4.4	CERTIFICATES.....	8
4.5	COMMUNICATION LAYER.....	8
5	TRAINING AND TESTING	9
6	COMPETENCE RULES	9
7	REGISTRATION PROCESS	10
7.1	TEST ENVIRONMENT.....	12
7.2	OPERATION ENVIRONMENT	12
8	DOCUMENTATION OF THE IS SERVICES AND CHANGES	13
9	HANDLING OF ERROR AND NON-STANDARD SITUATIONS	13
9.1	ALTERNATE WORKPLACE	14
10	CONNECTION SERVICE AVAILABILITY	14
11	ABBREVIATIONS USED	14
12	FINAL PROVISIONS	15

1 INTRODUCTION

This Executory Decree has been issued in conformity with Article 1 of the Rules of Operation of Centrálný depozitár cenných papierov SR, a.s. (hereinafter referred to as “Rules of Operation”), and defines details related to the communication of the participants with the information system of Centrálný depozitár cenných papierov SR, a.s. (CDCP).

The document describes technical options of the communication (hereinafter referred to as “connection service” with the information system (“IS”) of Centrálný depozitár cenných papierov SR, a.s. for its participants including related training, testing, and registration process agenda.

2 GENERAL VIEW



In Figure above

- IS CDCP is own information system of CDCP.
- ICP is a member of the central depository who uses IS CDCP services via his U2A and/or A2A interface. IS CDCP provides communication with T2S via T2S A2A interface. From T2S's point of view, this is an indirectly connected participant of the central depository (ICP).
- DCP is a member of central depository who uses direct connection with T2S as a participant of the central depository. From T2S's point of view, this is a directly connected participant of the central depository (DCP). For now, CDCP does not offer this option.

- PB is a payment bank that uses the direct connection with T2S as a participant of the national bank. From T2S's point of view, this is a directly connected participant of the national bank (DCP).
- VAS T2 are value added services of Target2 system the payment bank may use as an alternative to manage liquidity on cash account (DCA) in T2S.
- DCA is a cash account in T2S opened by the national bank in T2S for the payment bank.
- U2A/A2A T2S are interfaces of the T2S system.
- U2A/A2A CDCP are interfaces of the IS CDCP. The following chapters of this document describe the IS CDCP and its interfaces.

3 OPTIONS OF CONNECTION TO THE IS CDCP

1. Each participant of CDCP will decide how to connect to and communicate with the IS. CDCP offers the following options for the IS connection:
 - in single operation environment,
 - and at least one test/training environment.
2. The IS offers connection in two modes A2A and U2A. The participant may select from either one or both connection modes. Both modes are available in operation and test environment.
3. CDCP operates multiple test environments, and the participants have usually accessible just one.

3.1 U2A MODE

1. The U2A mode between the IS and participant is based on a web application available via a URL address in a browser via standard HTTPS and TLS protocol. The protocol must be permitted on the terminal computer and network components of the participant.
2. A client digital certificate (X.509) has been used for identification and authentication of the final user of the participant. The certificate should be issued by an accredited certification authority for the end user of the participant (certificate for a natural person), and the private key should be installed on his/her terminal computer. The public key should be registered in the IS and assigned to the participant for the U2A mode.
3. The IS communication server is identified by a server digital certificate.

3.2 A2A MODE

1. The A2A mode between the IS and participant is built on XML message exchange between the IS and the participant's information system. XML messages are based on ISO20022 standard and supplemented with proprietary elements and messages needed for the national market. For description of the A2A interface and XML messages, refer to a specific document available from CDCP website.
2. Technically, the A2A mode is made available via two communication channels:
 - IS web services,
 - SWIFT international communication system.
3. Structure of the XML messages is identical for both channels.
4. A client digital certificate (X.509) has been used for identification and authentication of the participant. The certificate should be issued by an accredited certification authority for the participant (certificate for a legal person), and the private key should be installed on a computer of the participant who operates its IS and communicates with the IS. The public key should be registered in the IS and assigned to the participant for the A2A mode.
5. The IS communication server with the web services is identified by a server digital certificate.

4 TECHNICAL REQUIREMENTS FOR THE PARTICIPANT

Technical requirements for available connection modes and communication with the IS that the participant has to meet are specified thereafter. The IS shall process all requests delivered by the participant in the U2A or A2A mode equally.

4.1 U2A MODE

1. The IS web application for the U2A mode generates pages in XHTML 1.0 language, which is supported by all commonly used Internet browsers (Internet Explorer, Mozilla Firefox, Google Chrome, Opera).
2. The IS web application does not require installation of any software from CDCP by the participant. The end computer of the user and his/her browser must be however configured to allow
 - installation and availability of the certificates for internet browser,
 - client Java script,
 - cookies,

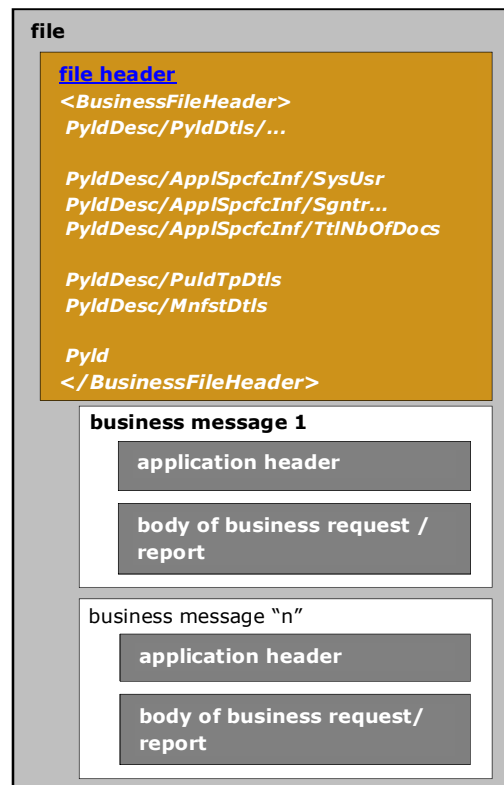
- functional Java applet add-ons, which requires installation of JRE on the user’s end computer.
3. Considering things mentioned above and fact that the latest versions of some Internet browsers disable use of the Java applet add-ons on the website, the real availability of the Internet browsers for the IS is limited to Internet Explorer and Mozilla Firefox. Supported is the latest version of the browser and two prior versions.
 4. The IS web application may print the screens using standard features of the Internet browser/OS and export of contents from some screens to text or XLS files also through standard services of the Internet browser.
 5. The IS web application has no special requests for the user’s end computer and therefore, the user may use for communication with the IS in the U2A mode any standard, modern PC with at least 1024x768 pixels screen (higher is better), keyboard, and mouse.

4.2 THE A2A MODE – WEB SERVICES

1. The IS publishes two web services with defined operations. The first web service allows to send an independent message to the IS and get a response from the IS. The second web service allows to send a batch of multiple messages in a file to the IS. The IS shall respond to the participant individually regardless how the message was received (separate message or file with multiple messages).
2. The first web service uses the secured communication technology Microsoft Windows Communication Foundation 4.5 (WCF) at the message level (“message security”). During communication the messages are exchanged in format of the A2A interface. A caller is identified by a client certificate.

<pre><AppHdr> Fr/FIIId/FinInstnId/BICFI To/FIIId/FinInstnId/BICFI BizMsgIdr ... </AppHdr></pre>	application header	complete A2A business request/report
<pre><Document> ... (e.g. sese.023) </Document></pre>	body of business requests/report	

3. Application header must contain a digital signature of the message despite intactness of the delivered message and sender's identification is provided also by the WCF infrastructure itself.
4. The second web service uses the secured communication technology Microsoft Windows Communication Foundation 4.5 (WCF) at the transport level ("transport security") where the communication is encrypted by SSL server certificate of the IS. A caller is identified by a client certificate.



5. File header must contain a digital signature. In this case no digital signature at the level of application headers of each message is required.

4.3 A2A – SWIFT MODE

1. For SWIFT message exchange, rules applied to the web services apply to the format of messages. After the participant delivers the message to CDCP's BIC code via the SWIFT network, the message will be processed in IS identically to the message delivered via the web services.

2. The IS shall respond with XML messages according to description of the A2A interface of CDCP.
3. Should the message from the participant delivered to the IS not comply with the IS requirements and description of the A2A interface, it is rejected automatically from processing, and admi.007 message is sent to the participant.

4.4 CERTIFICATES

1. Identification and authentication of the participant is ensured by digital certificate installed in the participant's computer. CDCP recommends to the participant that reasonable security action be adopted to protect the private key of the user/participant against discrediting. CDCP recommends installation of the certificate in a manner that requires entering of a solid password in each use.
2. CDCP shall not be liable for any loss, direct or indirect damage due to discrediting of the private key of the user/participant. If the participant is suspicious about the discrediting of his/her private key, the CDCP employees must be informed immediately to disable access of said user/certificate in the IS.
3. For the purposes of secured communication between the IS and the participant, it is necessary to register certificate public key in the IS, to include it to the correct group of the users, and assign the rights. To this end the participant submits the certificate's public key to an employee of CDCP. Each certificate may be registered once only in the IS.
4. The certificate may be used in the IS from the first until the last day of validity specified by the certification authority at issuance of the same.
5. If the participant is interested in use of a certificate issued by a certification authority of which use is not experienced in operation of the IS, the participant informs CDCP in advance about this interest, and correct operation of the certificate is checked in the IS test environment upon mutual agreement. Based on the test results CDCP informs the participant about ability/inability to use the certificate in the IS operation environment.

4.5 COMMUNICATION LAYER

1. For both communication modes, connection via Internet and reserved lines are available, and for A2A mode also SWIFT. Technical details and functional tests of the communication layer should be communicated in advance with the specified employees of CDCP.

5 TRAINING AND TESTING

1. CDCP allows the participants to attend training on use of the IS web application. Training organized by CDCP is not mandatory for the participants. Training of the participant's users may be provided by CDCP upon request of the participant, or participant may train on the "train the trainer" principle.
2. If the participant requires training organized by CDCP, the participant submits a request to CDCP. The training days are agreed between CDCP and the participant.
3. Should there be more extensive changes to the IS web application, CDCP stipulates training days well in advance and in sufficient extent prior to implementing the changes to the operation environment.
4. CDCP requires certification tests for the participants. The certification tests grant a sufficient level of surety to CDCP that the participant is ready for communication with the IS in the operation environment in the mode selected by the participant.
5. The participant informs CDCP about certification test results in the form of certification test results report. The certification test procedure and report on the test results are described in a specific document.
6. CDCP shall check each report on result of certification test of the participant and based on the result it shall decide to issue or not to issue the certificate, which demonstrates that the participant completed the certification tests in selected scope.
7. The certification process at the participant is not limited by CDCP to the certification testing, i.e. each participant may conduct in-house testing to the extent reasonable for his business needs.
8. In case of change to the IS, CDCP may require the participants to attend the testing of the changes, and require mandatory testing of the involved services or parts of the IS, and condition the entry of the participant to the operation environment following deployment of the changes.

6 COMPETENCE RULES

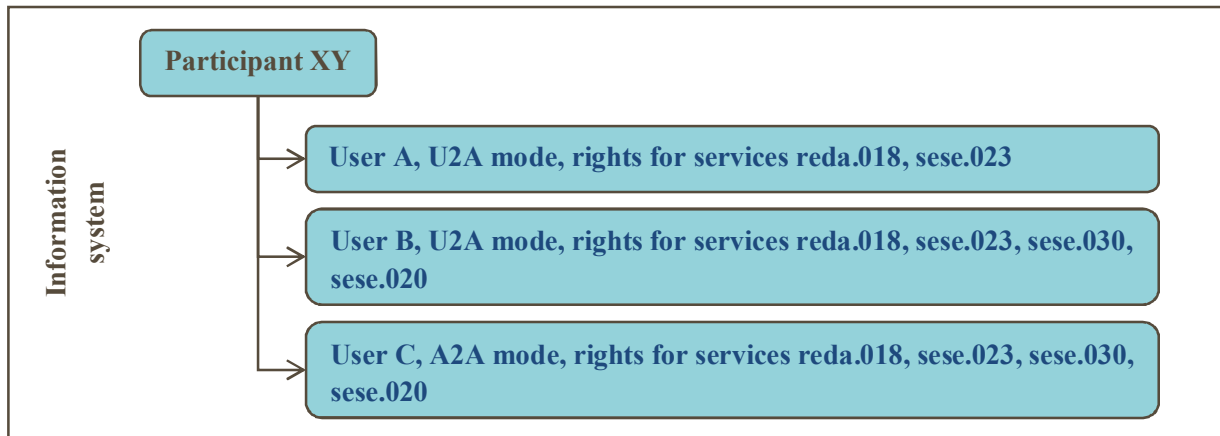
1. The participant shall be liable to CDCP for making access to trained users to the IS web application only.
2. The participant shall be liable to CDCP for using of own certified information system only in the A2A mode of connection, i.e. only an information system of the participant that successfully passed the certification tests, and can communicate with the IS in the A2A mode.

3. CDCP shall appoint “sponsors” with competences to deal with the issues and problems associated with the operation and use of the IS. The sponsors provide communication with the participant in the area of use of the IS, in particular:
 - keeping the records of contact persons of the participant responsible for use of the IS,
 - reviewing of the participant’s certification test results, and keeping records thereof including the issued certificates (certificate on the participant’s test result),
 - collection and primary processing of comments and impulses of the participant’s users of the IS,
 - communication of changes to the IS to the participants,
 - organizational support of the IS testing for the participants,
 - the IS web application user training,
 - dealing with error and non-standard events in the IS, communication to the participants.
4. The CDCP’s sponsor keeps records of the IS users per participant based on a registration process.
5. The participant appoints a contact person on his side for cooperation with the sponsors of CDCP to deal with the issues and problems related to the use of the IS, e.g. cooperation in organizing of the participant’s testing, cooperation in registration/exchange of certificates and configuration of user rights.
6. CDCP and the participants shall inform each other about e-mail addresses and phone numbers of the CDCP sponsors and contact persons of the participant for fulfilment of the tasks defined herein.
7. Communication of the CDCP sponsors and contact person of the participant takes place via e-mail messages for the reasons of operating flexibility. Both parties acknowledge that the e-mail communication may subject to monitoring. Should transfer of confidential information be needed, both parties shall apply an asymmetric encryption of the e-mail communication using the digital certificates.

7 REGISTRATION PROCESS

1. In order to get an access to some of the IS environment a registration process is mandatory for the participant. The purpose of the registration process is making sure the access of the participants to the IS is under control. The registration process has multiple steps.

2. The first step is registration of the participant in the IS environment. To this end, the participant submits “Request for registration/change to the IS CDCP participant’s registration” to CDCP where the required IS environment is identified in addition to his identification data.
3. If the participant intends to use or test the settlement of DVP instructions via DCA accounts or auto-collateralization in T2S, a request must be delivered to CDCP to link his accounts in which the securities are kept or to link CDCP accounts in which the securities are kept with his DCA account(s), whereas the link is established based on form “Securities Account Identification for Auto-collateralization” and configuration of the link to a dedicated cash account, and based on form “Payment Bank Consent to Identify the Securities Account for Auto-collateralization” and configuration of the link to the dedicated cash account.
4. Another step is registration of a specific user of already registered participant in the IS environment. The participant either once or repeatedly asks for the registration of an user of the IS by submission of the “Request for user registration in IS CDCP” form where identification data of the participant, required environment, communication method, certificate serial number, and required rights for services for the operation environment are defined.
5. The participant does not fill in the required service right in the request for user registration in the IS test environment. CDCP shall automatically grant rights to all services available to the participant.
6. CDCP does neither specify maximum nor minimum number of the registered users of the IS for a participant in any IS environment.
7. Should there be a need to change the already granted service rights for the IS user in the operation environment, the participant asks for registration of the IS user by filling in a request that replaces the prior one thereby.
8. Registration of the IS user is cancelled based on the form titled “Request for cancellation of registration of the IS CDCP user” filled in by the participant.
9. All accesses of the participants to the IS test environment granted prior to effective date of this document shall be regarded valid, and no additional registration process is needed.



In Figure above in an example of the participant XY and three users of the participant registered the IS. The users A, B in the U2A mode, and user C in the A2A mode. The registration of the participant took place based on the Request for participant registration in IS, and registration of the users based on three Requests for user registration in IS.

7.1 TEST ENVIRONMENT

1. The conditions for registration of the participant in the test/training environment of the IS are:
 - decision of CDCP about accepting a person as a participant in the sense of the provisions of the Rules of Operation of CDCP,
 - or formally expressed interest of a person to be a future participant of CDCP and signing of a Test Contract.
2. Conditions for registration of the user in the test/training environment of the IS are:
 - successful registration of a participant in the test environment.

7.2 OPERATION ENVIRONMENT

1. The conditions for registration of the participant in the operation environment of the IS are:
 - decision of CDCP about accepting a person as a participant in the sense of the provisions of the Rules of Operation of CDCP,
 - and also confirmed successful completion of the CDCP certification tests.
2. The conditions for registration of the user in the operation environment of the IS are:
 - successful registration of a participant in the operation environment,

- rights required for the user do not exceed the extent of the certification tests completed by the participant to date, in relevant mode (U2A, A2A).

8 DOCUMENTATION OF THE IS SERVICES AND CHANGES

1. Documentation for the IS services for the A2A mode is available for the participants from CDCP website. The user guide for the U2A mode is permanently available from menu in the IS web application.
2. The participants are authorized to make local copies of the IS documentation for their personal needs including the communication needs with their suppliers (e.g. IT services).
3. In case to changes to the IS services, CDCP publishes updated documentation on its website, deploys changes to the test environment, and informs contact persons thereof by e-mail, usually within a reasonable deadline prior to deployment of the changes to the operation environment. CDCP shall have right either to reduce or increase the deadline depending on the extent of changes and upon discussion with the participants.
4. This does not apply in case of a repair of a serious defect found in the operation IS environment. In that case change to the XML message structure of the A2A interface is not usually needed, and CDCP may apply quick patch and reduce the time needed for installation of the patch in the test environment to minimum (“hot-fix”).

9 HANDLING OF ERROR AND NON-STANDARD SITUATIONS

1. In case of errors found in the IS or the connection service unavailability, the participant may use the error and failure reporting service available from a URL address specified and published at www.cdcp.sk. CDCP creates automatically access of the participant to said service during registration of the participant/user in the test/training environment of the IS. For procedure of reporting of the errors and failures, refer to a specific document.
2. Should the website mentioned above be not available, the error and failure reporting service is available on hotline@cdcp.sk or phone numbers published on the CDCP’s website.

9.1 ALTERNATE WORKPLACE

1. CDCP maintains in its premises an alternate workplace for the participants with at least one personal computer allowing the participant to communicate with the IS operation environment in the U2A mode.
2. The purpose of the alternate workplace is provide the participants alternate way of communication with the IS in the U2A mode in case of communication failure between the IS and participant's premises/system.
3. If needed, the participant must ask CDCP for use of the CDCP alternate workplace. The workplace is made available upon agreement and in cooperation with CDCP and in addition, installation of the private key of the participant's user certificate must be made by the participant.
4. The alternate workplace does not serve to testing of the IS by the participant.

10 CONNECTION SERVICE AVAILABILITY

1. The connection service to the IS is accessible in conformity with the operation schedule and operation day of the T2S system.
2. In case of an exceptional event CDCP reserves right to limit availability of the connection service to the IS for the participants. The participants shall be informed about any such event usually in advance or afterwards depending on the cause and severity of the extraordinary event.

11 ABBREVIATIONS USED

Abbreviation	
URL	Uniform Resource Identifier
JRE	Java Runtime Environment
XML	Extensible Markup Language
A2A	Application to application
U2A	User to application
DCA	Dedicated Cash Account
DCP	Directly Connected Participant
ICP	Indirectly Connected Participant
VAS	T2 Value Added Services

12 FINAL PROVISIONS

1. This Executory Decree to the Rules of Operation enters into force on the day of approving thereof by the board of CDCP on 13 June 2017 and is effective from 3 July 2017.